Presented at the Institute of Navigation National Technical Meeting January 29, 2002

Intelligent Waterway System and the Waterway Information Network

J. W. Spalding, K. M. Shea, *U. S. Coast Guard Research & Development Center, Groton, CT*
M. J. Lewandowski*, Potomac Management Group, Groton, CT*

BIOGRAPHY

Mr. Joseph Spalding is a program area manager at the US Coast Guard R&D Center. Past efforts include development of Coast Guard DGPS technology. He is a member of RTCM SC104 and IEC TC80 working groups on Integrated Navigation Systems and radionavigation receivers. He holds a Bachelors degree in Electrical Engineering from State University of New York Maritime College, Masters of Science in Computer Science from the University of New Haven and is a licensed Merchant Marine officer.

Ms. Kathleen Shea is a project manager at the US Coast Guard R&D Center. Past efforts include development of a web-based survey for users of the Aids to Navigation System. She also developed cost models for the Coast Guard's Aids to Navigation System. Other efforts have been implementations of a Coast Guard Reserve Training Assignment System and the Merchant Mariner Licensing & Documentation System. She holds a Masters of Science in Computer Science from the University of New Haven.

Mr. M. J. Lewandowski is a research analyst for Potomac Management Group at the Coast Guard Research and Development Center. He served as a Coast Guard officer for twenty years in a variety of positions. He has also been a marine operations-management consultant and steamship agency port operations manager. He is a graduate of the U. S. Coast Guard Academy.

ABSTRACT

The Coast Guard has begun a research effort called the Intelligent Waterway System. The goal of this effort is to improve the efficiency and effectiveness of maritime related functions through the application of information technology. This is being done through the efforts of several projects including automatic identification systems and augmented reality for navigation, as well as interagency efforts. The research effort that ties these together is the Waterway Information Network (WIN).

The basic concept of WIN is to create a network to facilitate distribution of marine transportation system information. It is based upon existing peer to peer and XML Internet technology. The system will allow users to connect directly to information providers, such as government agencies, port authorities, marine exchanges, and other private companies that make up the Marine Transportation System. The network would be comprised of government agencies and private industry that would be both users and providers of information. For WIN, it is important to involve the various maritime information providers in the creation of a tailored XML vocabulary we call the Maritime Information Markup Language (MIML). MIML would be the key development toward an automated maritime information infrastructure and facilitate a seamless network of providers and consumers of maritime information.

An effective infrastructure for exchanging information has been identified as a major performance gap within the Coast Guard and the maritime transportation industry. IWS/WIN will fill this gap and enable other solutions to be built on top of it.

INTRODUCTION

There is a clear and real need to improve the transfer of information in the Marine Transportation System (MTS). Present shortcomings include a reliance on paper-based systems, including navigation charts, local Notices to Mariners, and various Government forms dealing with vessel-entry and clearance; individual and distinct methods and procedures for submitting and disseminating information; and numerous marine electronic information devices and systems that are not part of a fully integrated system. Recent studies have concluded that development of an Intelligent Waterway System for the United States is necessary to keep pace with the continuing growth in the amount of waterborne commerce seen over the past decade and forecast for the future.

Various MTS users and stakeholders recognize the need for improvement in information transfer. Because of the diversity of MTS interests, the quick fixes that result are often extremely limited in the type of information transferred, and generally have a specific information provider-information user channel. This "stovepipe" effect is often unnecessarily duplicated. The concept of an Intelligent Waterway System is one where information transfer becomes more efficient, more accurate, and more timely.

We propose a network approach, taking advantage of existing Internet technology. To achieve the desired result, we expect to use a Peer-to-peer methodology of distributed content rather than an "information hub." Existing technology allows for content security and limited distribution where necessary to protect sensitive information. A new, content-based mark-up language will be the basis for information transfer and transfer protocol.

BACKGROUND

Two reports give impetus and direction for this effort. In a 1999 report to Congress, the U. S. Department of Transportation summarized information needs:

> "There is a need to develop information management systems and infrastructure to provide a wide range of planning, operations management, and administrative support tools. Information resources should ideally be configured, linked, referenced, and maintained to ensure that they:
>
> - are easily accessible,
> - are up-to-date and accurate
> - eliminate redundant data input from information contributors, and
> - allow for rapid and organized information retrieval by all MTS user groups"[1].

In 1999, the National Research Council (Marine Board) established the Committee on Maritime Advanced Info Systems "to identify systems and their infrastructures that could promote safe and effective vessel transits thru US ports"[2]. The Marine Board stated a specific vision of the future:

- "Highly accurate information will be available in various formats—electronic displays, by radio, or on the Internet.
- Real-time hydrographic and meteorological data [will be available].
- Tides, currents and Coast Pilot-type information will be published in hard copy and on the Internet and updated through electronic transmissions.
- All vessels will be equipped with AIS which will be linked with shore-based VTS systems in busy harbors."[2]

The Marine Board specifically noted, "***Standards for data exchange, component interfaces, and user interfaces with critical navigation systems are all essential for creating a uniform operating environment among all ports and waterways***"[2].

In response to these reports, and as the Coast Guard representative to the Interagency Committee on the Marine Transportation System (ICMTS), the Coast Guard Office of Waterways Management commissioned a study to investigate the existing base of maritime information resources and to determine the information needs of the MTS user community. The study, An Assessment of the Integrated Maritime Information System (IMIS) Concept as Applied to U. S. Ports and Waterways [3], provided a strategic overview of the integrated maritime information system concept as it is evolving in the U.S. by:

- "Assessing the current user requirements and expectations by system components,
- Investigating the range of projects and activities underway in this area,
- Identifying major stakeholders and their roles in such a system, and
- Identifying ways the Coast Guard can contribute to and facilitate this concept"[3].

Three data gathering efforts were done: discussions with Federal and private maritime information specialists, an Internet search of maritime information websites, and a targeted user survey. The website search results showed that the Internet is *already* extensively used to disseminate maritime information by many stakeholders. Almost every site links to other maritime information sites, e.g. CG to NOAA, to USACE, etc. From the number of "hits" recorded, large numbers of users are getting information from the various sites.

The study also identified information *desired* in a marine information system (Table 1, below). In addition to the details in the matrix, there was a clear indication from the private sector that a maritime "information hub" (i.e., a centralized, single point data center) was not desired, though there "is a clear need for coordination and collaboration between government and industry" in developing an information system (why the Coast Guard should be involved) [3].

The major thrust of the IWS R&D objective is to build and develop build a concept, tools and a prototype, then use this effort to leverage available technology and expand the Waterway Information Network to reach the wide range of marine information providers and users. The end goal is to improve security, safety & mobility of the MTS.

IWS/WIN REQUIREMENTS

The Marine Transportation System has an extremely diverse information community. There are numerous government entities and agencies: federal, state, local; military and non-military. There is a vast array of commercial, private, and recreational members of the MTS. A most important feature of this information community is that many stakeholders are both information providers and information users. Information has value, and some entities derive profit from providing that information or by adding additional value to publicly available information. Because of the nature of information, both providers and users require some level of security in the information flow. Finally, there is a need for minimal cost or some method of cost recovery.

Table 1

Desired Components, Availability, Operation and Maintenance, and Access Mode for a Marine Information System [3]

COMPONENTS	Availability		Operate and Maintain				Access Mode			
	Open	Proprietary	Federal	State	Port	Private/ MX	Real-time	Web	Voice	Hard Copy
METEOROLOGICAL INFORMATION										
Real-time Port Met/Ocean Data	X		X			X	**X**	**X**		
Coastal Weather Forecasts	X		X					X	X	
VESSEL STATUS INFORMATION										
Vessel Location and Navigation Information		X	X			X				
Cargo/Hazardous Cargo Onboard		X	X			X				
Port State Control Info	X		X					X		
Material Status of Hull and Machinery	X		X					X		
SAR and Medical Response Capability	X		X					X		
PORT INFORMATION										
Safety Advisories for Port and Approaches	X		X					X	X	
Maritime Regulations Applicable to a Port	X		X					X		X
Facilities and Services Available to Port Users						X		X		
Port Contacts and Reporting Requirements						X		X		
NAVIGATION INFORMATION										
Navigation Charts	X		X					X		X
Updates to Charts	X		X					X		X
Tide Tables	X		X					X		X
Coast Pilot	X		X					X		X
SHIP SAFETY AND RELIABILITY INFORMATION										
Vessel Casualty Data	X		X					X		X
Safety Incident Data	X		X					X		X
Hull and Machinery Reliability Data	X		X					X		X
Ship Safety and Reliability Advisories	X		X					X		X
RECREATIONAL BOATING INFORMATION										
USCG and State Boating Regulations	X		X					X		X
Small Boat Product Safety Advisories	X		X					X		
Recreational Boating Accident Database	X		X					X		X
COMMERCIAL FLEET, PASSENGER, AND CARGO TRACKING AND MANAGEMENT										
Directory of Commercial Vessels in Service	X		X			X		X		
Vessel Schedule Information		X				X		X		
Cargo Tracking Data		X				X		X		
Passenger Tracking Data		X				X		X		X
PORT AND WATERWAYS PLANNING AND MANAGEMENT										
Waterways Vessel Transit and Tonnage Statistics		X				X		X		
Port Characteristics and Facilities Data	X		X		X	X		X		
Shipping Industry Future Trends Data	X		X					X		
PORT EMERGENCY RESPONSE PLANS										
Oil and Chemical Spills Contingency Plans	X		X	X	X			X		X
Fire Response Plans	X		X	X	X			X		X
Storm / Hurricane Response/Evacuation Plans	X		X	X	X			X		X
Security Incidents Response Plans	X		X	X	X			X		X

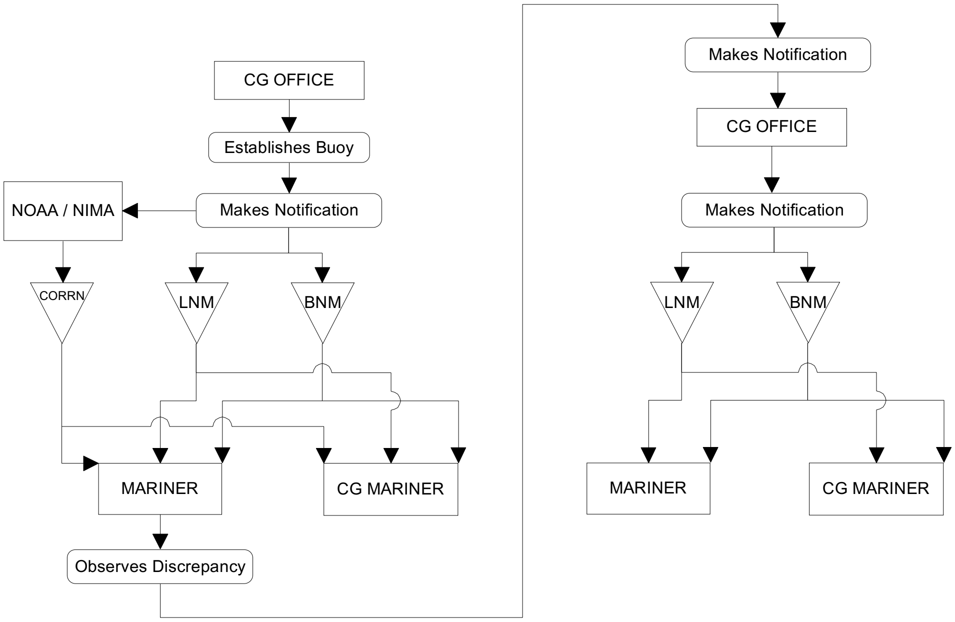
PRESENT MTS INFORMATION FLOW

We view the present marine information transfer arrangement as a multitude of information "stovepipes." Information providers transfer a single type of information through one or more methods to specific users in a set, well-bounded format. Some examples of these are the published Local Notice to Mariners, weekly summary Notice to Mariners, marine weather information broadcasts and the Physical Oceanographic Real-Time System. In these examples, multiple government agencies provide information to a wide range of information users, including elements of the government agencies themselves. The aforementioned could all be considered "public" information, broadcast, published, or accessible through the Internet. In all these cases, the information "providers" frequently rely upon the information "users" for updating the same information.

Consider a navigation buoy. At some point in time, it was determined that a buoy be placed in a location (say, to mark the beginning of a vessel traffic separation scheme). After the buoy is established, the Coast Guard notifies NOAA/NIMA for a chart correction (CORRN), while simultaneously advising mariners (including Coast Guard mariners) through the Broadcast and Local Notice to Mariners (BNM & LNM) process. Should the buoy suffer damage and sink, chances are that a mariner will then notify the Coast Guard that the buoy is not "on-station," i.e. at the charted position. In turn, the Coast Guard will then advertise that fact through a Broadcast Notice to Mariners or in a Local Notice to Mariners indicating the discrepancy. In this one example, elements of the Coast Guard act as information providers twice while as information users three times.

An equally large amount of information is transferred solely to various government agencies. A ship's agent notifies at least four federal agencies as to a vessel's arrival. The agent also must notify or arrange services with tugs, pilots, linehandlers, stevedores, terminalling, chandlering, and many others. Though in selected ports some of these functions are consolidated to some degree by "marine exchanges," there is still quite a bit of similar information being passed multiple individual times to multiple information users. Since the September 2001 terrorist attacks and an increased emphasis on port and maritime security, information transfer requirements have substantially increased.

Figure 1
Simplified Aids to Navigation Information Flow Process



THE FUTURE – A SCENARIO

Aboard the Motor Tanker Venturepower K, the 2nd Officer (2/O) has just notified the master that the vessel passed due south of the Davis South Shoal Buoy enroute the Bridgeport lightering zone in Long Island Sound.

With the vessel 70 miles from the Point Judith Pilot Station, in the past the 2/O would have been lining up a sequence of paper charts 13218, 13205, 13212, 12354, 12363 and 12369, even though the vessel would be traveling through an extremely small percentage of the area covered by each paper chart. Now, since the 2/O has already loaded the CD "Coastal Approaches and Inland Waters of North America, the United States, New York to Boston" the 2/O zooms out on the vessel's combined electronic chart display and radar repeater navigation screen and draws an approximate intended track with a finger. Rather than loading the digital equivalent of each chart's entire data base, and the duplicity found with paper chart overlap, the new navigation display processors only load the desired area, freeing up memory and processor activity.

As the vessel has lost about 2-hours time during the final leg of its voyage from Portugal, the 2/O updates the estimated time of arrival to pilot station by zooming in to the area between Block Island and Pt. Judith clicking on the "non-physical features" icon which draws a small, dashed, circle with the legend "Pilot Boarding Area" on the display. The 2/O touches the center of the circle, moves to the Navigation Features Drag-Down menu and touches "ETA (estimated time of arrival)." The 2/O then touches "Update External" and sends the revised ETA with vessel identification information to the owners, charterer, agent, pilot dispatcher and Coast Guard, well before the four-hour time limit to avoid incurring any pilot stand-by charges. The pilot dispatcher and agent immediately receive this info on their hand-held processors, set to the "page" mode. The Coast Guard dutystander also receives the update, and knows that the boarding party won't need to meet the launch to conduct the Tank Vessel/Certificate of Compliance exam for another twelve hours.

Since this is Venturepower K's first trip to the US in two years, diverted from a spot voyage to Montreal after completion of a time charter (Europe West Coast / West Mediterranean), the 2/O updates all required navigation information via satellite. Only navigation updates for the specific geographic area drawn on the screen are requested and retrieved from the database. Gone are the carriage requirements for Weekly Notices to Mariners and Monthly summaries, since this information is immediately updated, showing actual conditions, and available through redundant methods. The voice Broadcast Notices to Mariners have been long eliminated, replaced by digital navigation notice screen updates for urgent marine information and initial aids to navigation discrepancy reports. The second officer wasn't even in maritime school when his predecessors had to make due with receiving a stack of printed chart corrections and Admiralty templates, then making pen corrections to an entire portfolio of charts for an obscure channel marker known only to a myopic Port-State inspector.

Venturepower K is outfitted with automatic identification system (AIS), as are all vessels longer than 40 feet, and smaller vessels on a voluntary basis. This ship to ship, ship to shore, shore to ship system allows identification and tracking of other vessels, obviating much of the bridge-to-bridge chatter and confusion formerly heard on Ch 13 VHF-FM (bridge-to-bridge voice radio). The 2/O sees on the navigation and radar display that the sistership Ventureprima K is outbound Narragansett Bay headed south, thirty miles away, the only other transponder-equipped vessel around. The 2/O mentions to the helm-lookout that the last time they transitted these waters, there were numerous fishing boats, but none show on the navigation display, even though international agreement requires a simplified tracking transponder for fishing vessels in coastal waters. The 2/O quickly types a brief, informal message to the sistership giving their regards and attaches it as an "additional information" tag to the automatic identification system transponder signal, which will be seen only by the Ventureprima K.

Going on with business, the 2/O calls up the supplementary/temporary information overlay for the nav display. A white dashed block appears around the vessel's position with the legend "Area temporarily closed to mid-water and bottom fishing." The other item that catches his attention is the flashing white note to the west of the pilot boarding area advising of the Sound-off Club sailboat regatta today and tomorrow. Hopefully the pilot will board early to minimize maneuvering in the regatta venue.

The integrated navigation system plot of the vessel's track history and intended track show that the first of many transponder equipped "smart buoys" will be showing up as radar targets. The 2/O notes that one of the buoys shown on the nav display is flashing, indicating that it sensed itself outside of its watch circle and is also providing a real-time position update to vessels via the shore-based navigation update network. Because the buoy is off-station, the radar beacon (RACON) signal has automatically turned off. This RACON feature, one of the first "smart buoy" technologies from the 1970s, remains a useful tool for the smaller vessels not equipped with the newest developments in navigation equipment.

Since there is no other commercial vessel traffic, Venturepower K proceeds directly towards the pilot station. Another transponder-equipped vessel shows upon the display just north of Block Island. The ID "CT PILOT" with "INFO" tag appears. The 2/O touches the "INFO" tag, clicks, and sees a text message "board pilot E of Block Is, vsl stbd side, present course."

The 2/O then advises the Master and prepares to test maneuvering systems.

All this is possible because of the IWS and WIN.

A NETWORK APPROACH

We propose a fully-integrated, Internet-based network solution as an alternative to the present-day "stovepipe" information transfer process. The Waterway Information Network will emphasize distributed content, where each information provider retains control of its data, without having a centralized information hub. Though aspects of peer-to-peer information transfer will be used (information flow without central server pass-through), the network organization will have certain elements of server control. User registration and logon will be required, and secure Internet features will be used. Discussions among staff and potential information providers indicate this is an absolute requirement, particularly for controlling access, defining protocols and ensuring information security.

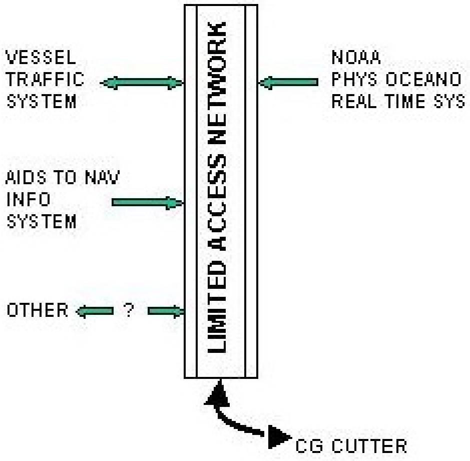
In the ISO Open Systems Interconnection Reference Model, WIN will rest in the **session** layer, above the **transport** layer and TCP/IP, but below the **presentation** layer and **application** layer [4]. The presentation layer, which serves to standardize data presentations to applications, will be addressed as the Maritime Information Markup Language (MIML). In this hierarchy, WIN will be readily accessible to the development of commercial application programs.

DISTRIBUTED CONTENT MANAGEMENT

The concept of distributed content management is sound for addressing the need to access information wherever it resides [5], but we feel it is important to maintain effective network control and information security, even when sharing information real-time within a distributed network of stakeholders. This is particularly important for information providers who require the highest degree of information integrity. The goal of the network is to seamlessly transfer information from providers to users, with the network providing the architecture, developing protocols, maintaining standards, while ensuring information integrity and a high degree of security, for both network and information sources.

A most basic model of a distributed content network solution follows (figure 2). In this example, we'll consider a network. This example could be considered a Local Area Network (LAN) or Intranet, but because we will be considering mobile sites and users, we'll call this first example a Limited Access Network. Information from three sources, available on the network would be available for processing by the user, in this case a Coast Guard cutter. Though two of the information sources shown are Coast Guard internal (NOAA's PORTS information is available by telephone or website), at present there is no network-based method for seamless information transfer to a Coast Guard cutter's shipboard command and control system (electronic charting, radar, and navigation suite). We envision a system that would allow automatic query and information retrieval, albeit in this way, the network seems to retain a client-server appearance.

Figure 2
Limited Access Network



Further development of our network solution will include multiple information sources and multiple information users. This is where the utility of the network will realize its greatest advantage. We could look at the network as a series of independent information providers and information users, but in reality, many of the information users are also information producers. The symbiotic (or interdependent) navigational information situation is such where most of the information user entities, particularly waterway users, contribute information updates to the original information "sources," and for the purposes of information transfer are sources themselves. This would address the reliance on paper flow as indicated in the earlier aid to navigation example.

PEER-TO-PEER NETWORK

The Waterway Information Network will meet information user and information provider needs through a derivation of a peer to peer structure. There are five peer-to-peer models as defined by Gartner [5]. **Atomistic** is considered the truest, involving peer-to-peer connectivity without a server. In this model there is no method to establish links based on data availability or user identity. In **user-centered** models, a directory provides the basis for peer connectivity (i.e. **Napster**). **Data centered** structure allows users to search and access other peers' data. **Web Mk 2** takes identity from a combination of features of the first three models. The first three models are integrated, with directory based user links. **Compute-centered** structured shares processing among users, with server coordination of the processing. WIN will essentially be a Web Mk 2 system [5]. A look at two existing peer-to-peer networks may be helpful in understanding network structure.

An early peer to peer application was **Napster**, which allowed sharing of large files (music files). The Napster application itself was more or less a "traffic-cop" (a server) that both gave directions (told prospective information users/clients where the desired information was available) and let the traffic flow (connected information users with information sources). It required centralized user registration and maintained a centralized content index (which led to its legal vulnerabilities).

Morpheus (MusicCity) is a newer file-sharing distributed network. Unlike Napster, Morpheus does not maintain a centralized content index and does not filter content. However, like Napster, Morpheus is formally a *closed* system, requiring centralized user registration and logon. Another major difference from Napster is that Morpheus supports transfer of audio, video, image, document and other software files, where Napster supported the sharing of only MP3 audio files [6]. Morpheus uses metadata to describe file content, allowing user searches by element or attribute tags.

As a user logs on (with appropriate peer authentication—closed system security), the server connects the peer to a supernode which acts as a search hub for all connected peers. The supernode furnishes the peer with the internet protocol address of another peer with the appropriate file, and then file downloads are strictly peer to peer [6]. Still another feature of Morpheus is the ability to track alternative peers with the same information files. Should connectivity or information transfer fail between an information user and information provider, file transfer can continue from another peer with that same file. At this stage of research, we expect WIN to function somewhat on the lines of Morpheus.

SECURITY AND THE WATERWAY INFORMATION NETWORK

Security is of vital importance to a network-based system that will provide information for operational and safety decisions. The Waterway Information Network will be used as a system that allows various government entities to review information and derive knowledge concerning port safety and security concerns, while at the same time, different commercial entities will be able to coordinate time-critical activities and apply up-to-date information for navigational situation awareness. As a relatively open (but requiring peer registration), distributed network of numerous maritime information providers and users, WIN will have its own unique challenges. Above all, stakeholder acceptance, and their use of WIN to submit information, will only occur if the stakeholders are confident that their information is secure.

As an Internet-based application, Internet security issues apply. **Eavesdropping** is when information privacy is compromised. Though WIN will not be configured for classified information, other types of proprietary or sensitive information may be passed, for example, shipping or personal information. **Tampering** occurs when information is modified or replaced. For example, someone could alter vessel arrival times to improperly gain a preferred berthing, or modify a navigation chart update to show incorrect information. **Impersonation** occurs when an entity poses as the intended recipient or an information provider. "Spoofing" occurs when an entity pretends to be something or someone it's not and sets itself up as an "illegitimate" site.

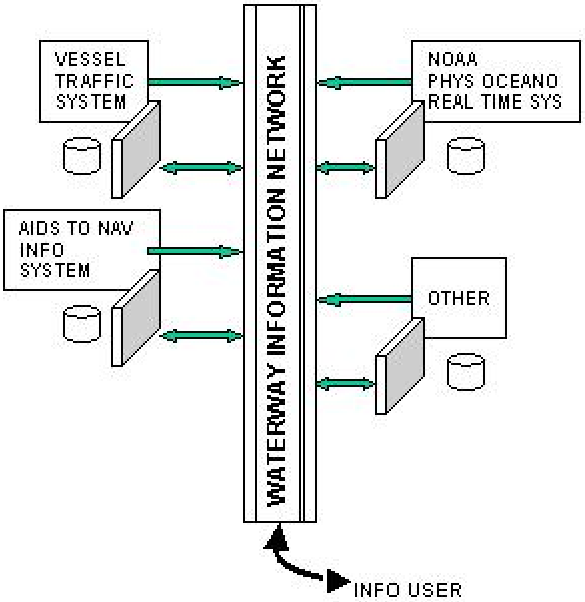
Commercial, off-the-shelf resources are available for Internet security which protect a network from these abuses. They follow a well-established set of standards called "public-key cryptography." Public-key cryptography provides **encryption and decryption**. This allows communicating parties to digitally mask information sent to each other. The sender encrypts, or scrambles, information before sending it. The receiver decrypts, or unscrambles, the information after receiving it. While in transit, the encrypted information is unintelligible to an intruder. Public-key cryptography also provides **tamper detection** and **authentication,** that is, verification that information in transit has not been modified and confirmation of a sender's actual identity [7].

WIN will use Transport Layer Security (TLS) based on Secure Sockets Layer (SSL) protocol [8]. TLS protocol runs above the Transport Control Protocol/Internet Protocol governing transport and routing of data over the Internet, but below higher level protocols as HTTP or Lightweight Directory Access Protocol [9]. WIN will use a Wireless Transport Layer Security (WTLS) with Wireless Access Protocol (WAP) for devices not actually connected to the Internet [10].

Transport Layer Security server authentication allows a user to confirm a server's identity while client authorization allows the server to confirm the user's identity. Because of occasional sensitive information passing, WIN will also incorporate an encrypted TLS connection. Digital certificates issued by a Certification Authority (CA) will provide unique identifiers and allow secure communication [8]. In addition to common Internet CAs, WIN will also incorporate wireless digital certificates [10].

Most WIN peers will use both server and client certificates. When Transport Layer Security is activated, both authentications create secure information transfer means either to or from the peer. We also expect that some entities may want or require additional security of information. WIN will support encryption to the same degree of existing private digital nets. As a final degree of protection, we fully expect data sources to not allow direct user access to their databases. As the accompanying schematic (figure 3) shows, we expect the WIN application to be distinctly separate from the source's actual database, with the information provider mirroring the actual database elements it want to disseminate or allow access to, at the WIN application level.

Figure 3
WIN Schematic
Firewalls prevent direct user access to actual data



WIN will have various layers of information access and availability. Entities on WIN may be information providers or information users, but we expect that most will be both providers and users. Some users might have a higher level of access to information, whether by a commercial, proprietary arrangement (subscription service) or as federal agencies with statutory authority. The tools available today can provide the degree of security needed to ensure integrity and privacy of information over the distributed network.

MARITIME INFORMATION MARKUP LANGUAGE (MIML)

The Waterway Information Network will need the ability to identify and process extremely large amounts of information of various types and various formats. One of the first steps in the development of this network is the identification or creation of a language that facilitates automated exchange of communications between maritime information providers and users. Electronic navigation chart information updates will likely use the existing International Hydrographic Organization (IHO) standard S-57. Information for Notices to Mariners already exists in text format. Weather information is in text and graphics. A mechanism for applying the varied formats and types of information in a consistent manner is necessary.

The information technology industry has developed an enabling technology, Extensible Markup Language (XML), which is designed for exchanging information in such a network. Many industries are developing tailored versions of XML that are information category specific. Manufacturing supply-chain management, including ordering, purchasing, shipping and tracking is one industrial application that has a great degree of information-type commonality. The marine community, though extremely diverse in information requirements, also lends itself to development of a "common" language. For WIN it will be important to involve the various information providers in the creation of this tailored XML, which we are tentatively calling the Maritime Information Markup Language (MIML). With development of the MIML, a coincident effort will be undertaken to identify and develop protocols and standards for language use and information transfer.

Arizona State University has begun a preliminary effort of creating a new markup language under the auspices of a National Science Foundation grant in collaboration with NOAA and the Coast Guard [11]. The initial goal is to create a computational ontology that can facilitate effective sharing of maritime information. Initial data consists of electronic charts from NIMA, and NOAA and text files of the existing Coast Pilot from NOAA. A demonstration information retrieval application is presently available [11]. Future action will include forming a MIML working group (consortium) as a venue for protocols and standards. As interest grows, we will promote and encourage participation by both government and private concerns. Though the scope of this undertaking is rather large, we are hopeful that with coordination and collaboration, the maritime community finds the Waterway Information network a worthwhile endeavor, and becomes a full partner with us.

As with anything new, user participation and customer "buy-in" is necessary. Early in the development phase, we plan to conduct focus groups, workshops, and/or other information gathering processes to further develop the interest and interaction with Federal agency partners and fellow information providers. Each provider of maritime information will be recruited to join this effort and help in developing the data structure and data dictionary parts of the MIML that would pass their data.

CONCLUSION

Effective, efficient information exchange with the maritime public and among government agencies is key to closing performance gaps in several areas of marine and navigation safety and port security. There is no standard method to transfer, share, and improve the timeliness of waterway relevant information within, federal, state, port, shipping, and recreational vessel communities. To meet the ever-changing needs of maritime commerce, recreational boaters, and government agencies, the Coast Guard R & D Center is spearheading an effort to make maritime transportation information available through the Internet. This is an excellent “e-government” opportunity to improve services and provide a superior product that plays an important role in the evolution of navigation. Current technological developments combined with existing partnership opportunities and stated Department of Transportation objectives make this an ideal project to pursue.

REFERENCES

[1] U. S. Department of Transportation. (1999). *An Assessment of the U. S. Marine Transportation System, A Report To Congress*. Washington, DC. U. S. Department of Transportation.

[2] Committee on Maritime Advanced Info Systems, Marine Board, Commission on Engineering and Technical Systems, National Research Council. (1999). *Applying Advanced Information Systems to Ports and Waterways Management*. National Academy Press.

[3] U. S. Coast Guard Office of Waterways Management (G-WM) /Potomac Management Group (PMG). (2001). *An Assessment of the Integrated Maritime Information System (IMIS) Concept as Applied to U. S. Ports and Waterways*. (Contract No. DTCG23-00-D-MM3A01). Alexandria, VA.

[4] Tanenbaum, A. S. (1998). *Computer Networks*. Englewood Cliffs, NJ: Prentice Hall

[5] Gartner Consulting. (2001). *The Emergence of Distributed Content Management and Peer-to-Peer Content Networks, Engagement #010022501*. GartnerGroup, San Jose CA.

[6] Truelove, K. and Chasin, A. (2001, July 2). *Morpehus Out of the Underworld*. The O’Rielly Network, http:/ www.oreilly.com/pub/a/p2p/2001/07/02morpheus.html.

[7] Netscape. (1998). *Introduction to Public-Key Cryptography*. http://developer.netscape.com/docs/ manuals/security/pkin.htm.

[8] Netscape. (1998) *Introduction to SSL*. http:// developer. netscape.com/docs/manuals/security/sslin/htm.

[9] SearchSecurity.com. (2001, June 20). *Transport Layer Security*. http://searchsecurity.techtarget.com/ sDefinition/ 0,,sid14_gci557332,00.html.

[10] Macphee, A. (2001, January). *Understanding Digital Certificates and Wireless Transport Layer Security (WTLS)*. Entrust, Inc. http://www.entrust.com/ resources/whitepapers.htm.

[11] Malyankar, R. M. (2002, January) *Elements of Semantic Web Infrastructure for Maritime Information*. Paper presented at the Institute of Navigation National Technical Meeting, San Diego, CA.